A note on the dual codes of module skew codes

Delphine Boucher, Félix Ulmer

▶ **To cite this version:**

Delphine Boucher, Félix Ulmer. A note on the dual codes of module skew codes. Liqun Chen. Cryptography and coding: 13th IMA international conference, IMACC 2011, Oxford, UK, December 12-15, 2011 : proceedings, Springer, pp.230-243, 2011, Lecture Notes in Computer Science, vol. 7089, 978-3-642-25515-1. 10.1007/978-3-642-25516-8_14 . hal-00602796v2

HAL Id: hal-00602796
https://hal.science/hal-00602796v2

Submitted on 6 Sep 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A note on the dual codes of module skew codes

D. Boucher and F. Ulmer *

September 4, 2011

Abstract

In [4], starting from an automorphism θ of a finite field $\mathbb{F}_q$ and a skew polynomial ring $R = \mathbb{F}_q[X;\theta]$, module θ-codes are defined as left R-submodules of R/Rf where $f \in R$. In [4] it is conjectured that an Euclidean self-dual module θ-code is a θ-constacyclic code and a proof is given in the special case when the order of θ divides the length of the code. In this paper we prove that this conjecture holds in general by showing that the dual of a module θ-code is a module θ-code if and only if it is a θ-constacyclic code. Furthermore, we establish that a module θ-code which is not θ-constacyclic is a shortened θ-constacyclic code and that its dual is a punctured θ-constacyclic code. This enables us to give the general form of a parity-check matrix for module θ-codes and for module (θ,δ)-codes over $\mathbb{F}_q[X;\theta,\delta]$ where δ is a derivation over $\mathbb{F}_q$. We also prove the conjecture for module θ-codes who are defined over a ring $A[X;\theta]$ where A is a finite ring. Lastly we construct self-dual θ-cyclic codes of length 2^s over $\mathbb{F}_4$ for $s \geq 3$ which are asymptotically bad and conjecture that there exists no other self-dual module θ-code of this length over $\mathbb{F}_4$.

1 Introduction

Starting from the finite field $\mathbb{F}_q$ and an automorphism θ of $\mathbb{F}_q$, a ring structure is defined in [7] on the set:

$$R = \mathbb{F}_q[X;\theta] \,=\, \{a_n X^n + \ldots + a_1 X + a_0 \,|\, a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\}\,.$$

The addition in R is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X \cdot a = \theta(a)\, X$ $(a \in \mathbb{F}_q)$ and extended to all elements of R by associativity and distributivity. The ring R is called a skew polynomial ring and its elements are skew polynomials. It is a left and right Euclidean ring whose left and right ideals are principal (cf. [4]). In the following we denote $(\mathbb{F}_q)^\theta$ the fixed field of θ in $\mathbb{F}_q$.

Following [4] we define linear codes using skew polynomial rings $\mathbb{F}_q[X;\theta]$.

Definition 1 *Consider $R = \mathbb{F}_q[X;\theta]$ and let $f \in R$ be of degree n. A* module θ-code *(or module skew code) $\mathcal{C}$ is a left R-submodule $Rg/Rf \subset R/Rf$ in the basis $1, X, \ldots, X^{n-1}$ where g is a right divisor of f in R. The length of the code is $n = \deg(f)$ and its dimension is $k = \deg(f) - \deg(g)$, we say that the code $\mathcal{C}$ is of type $[n,k]_q$. If the minimal distance of the code is d, then we say that the code $\mathcal{C}$ is of type $[n,k,d]_q$. We denote this code $\mathcal{C} = (g)_{n,\theta}$. If there exists an $a \in \mathbb{F}_q^*$ such that g divides $X^n - a$ on the right then the code $(g)_{n,\theta}$ is* θ-constacyclic. *We will denote it $(g)^a_{n,\theta}$. If $a = 1$, the code is* θ-cyclic *and if $a = -1$, it is* θ-negacyclic.

*IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

For $g = \sum_{i=0}^{n-k} g_i X^i$, the generator matrix of a module θ-code $(g)_{n,\theta}$ is given by $G_{g,n,\theta} =$

$$\begin{pmatrix} g_0 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \cdots & \theta(g_{n-k-1}) & \theta(g_{n-k}) & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \cdots & 0 & \theta^{k-1}(g_0) & \cdots & \theta^{k-1}(g_{n-k-1}) & \theta^{k-1}(g_{n-k}) \end{pmatrix}$$

In this paper we will always assume that the constant term g_0 of g is nonzero. According to the above generator matrix, this is not a strong restriction, since it is equivalent to the fact that the first entry of a code word in $(g)_{n,\theta}$ is not always zero.

Note that the skew polynomial f does not appear in the generating matrix, but that divisibility properties in the noncommutative ring $R = \mathbb{F}_q[X;\theta]$, which is not a unique factorization ring, determine most properties of the module θ-code Rg/Rf. In particular the code $\mathcal{C} = (g)_{n,\theta}$ is θ-constacyclic if and only if there exists an $a \in \mathbb{F}_q^*$ such that g is a right divisor of $X^n - a$ in R.

The material is organized as follows. In section 2, we characterize the θ-constacyclic codes in terms of their group of semi-linear automorphisms (Proposition 1) and establish that a module θ-code which is not θ-constacyclic is a shortened θ-constacyclic code (Proposition 2). In section 3, we show that the dual of a module θ-code is a module θ-code if and only if it is a θ-constacyclic code (Theorem 1). As a consequence (Corollary 1), we prove the conjecture given in [4] which states that an Euclidean self-dual module θ-code is a θ-constacyclic code. Furthermore, we establish that the dual of a module θ-code which is not θ-constacyclic is a punctured θ-constacyclic code (Proposition 3). This enables us to give the general form of a parity-check matrix for module θ-codes (Corollary3) and to extend this result in section 4 to module (θ, δ)-codes over $\mathbb{F}_q[X;\theta,\delta]$ where δ is a derivation over $\mathbb{F}_q$ (Corollary 4). In section 5, we show that the conjecture remains true for module θ-codes who are defined over a ring $A[X;\theta]$ where A is a finite ring (Corollary 5). In the last section, we construct self-dual θ-cyclic codes of length 2^s over $\mathbb{F}_4$ for $s \geq 3$ which are asymptotically bad (Theorem 2) and conjecture that there exists no other self-dual module θ-code of this length over $\mathbb{F}_4$.

2 Some remarks about module θ-codes

For a θ-constacyclic code $(g)_{n,\theta}^a$ we have

$$(c_0, \ldots, c_{n-1}) \in (g)_{n,\theta}^a \Rightarrow (a\,\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in (g)_{n,\theta}^a.$$

The following proposition characterize a θ-constacyclic code in terms of its group of semi-linear automorphisms.

Proposition 1 *A module θ-code is a θ-constacyclic code if and only if it is invariant under the semi-linear map $\sigma_a \circ \Theta$, where $\Theta : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is defined by $\Theta((c_0, \ldots, c_{n-1})) = (\theta(c_0), \ldots, \theta(c_{n-1}))$, $a \in \mathbb{F}_q^*$ and σ_a is an $\mathbb{F}_q$-linear map of $\mathbb{F}_q^n$ whose matrix is*

$$\begin{pmatrix} 0 & \cdots & 0 & 0 & a \\ 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

PROOF. If the code is a θ-constacyclic code $(g)^a_{n,\theta}$, then we have $\sum_{i=0}^{n-1} c_i X^i \in Rg/R(X^n-a)$ implies

$$X \cdot \sum_{i=0}^{n-1} c_i X^i = \theta(c_{n-2})X^{n-1} + \ldots + \theta(c_0)X + a\cdots\theta(c_{n-1}) \in Rg/R(X^n-a)$$

showing that the code is invariant under $\sigma_a \circ \Theta$.
Conversely if a module θ-code $\mathcal{C}$ corresponding to Rg/Rf is invariant under $\sigma_a \circ \Theta$, then for

$$c = \sum_{i=0}^{n-1} c_i X^i \in Rg/Rf$$

both $\sigma_a \circ \Theta(c_0, \ldots, c_{n-1}) = (a\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2}))$ and the code word corresponding to $X \cdot c$ belong to $\mathcal{C}$. Therefore

$$X \cdot c - \big(\theta(c_{n-2})X^{n-1} + \ldots + \theta(c_0)X + a\theta(c_{n-1})\big) = \theta(c_{n-1}) \cdot (X^n - a) \in Rg/Rf$$

Since $g_0 \neq 0$ there exists a code word with $\theta(c_{n-1}) \neq 0$, showing that $X^n - a$ belongs to Rg/Rf. Therefore f is a right divisor of $X^n - a$, and since both are of degree n they must differ by a constant multiple. We obtain that $Rg/Rf = Rg/R(X^n-a)$ showing that $\mathcal{C}$ is the θ-constacyclic code $(g)^a_{n,\theta}$. ∎

We will need the following classical notion for linear codes:

Definition 2 *Let $\mathcal{C}'$ be a $[n', k']$ linear code over a finite field $\mathbb{F}_q$ and let $n \in \mathbb{N}^*$ be such that $n < n'$. A code $\mathcal{C}$ of length n is*

- *a* shortened *code of $\mathcal{C}'$ if*

$$\mathcal{C} = \rho_{n' \to n}(\mathcal{C}') := \{c \in \mathbb{F}_q^n, (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in \mathcal{C}'\}$$

- *a* punctured *code of $\mathcal{C}'$ if*

$$\mathcal{C} = \pi_{n' \to n}(\mathcal{C}') := \{c \in \mathbb{F}_q^n, (c_0, \ldots, c_{n-1}, c_n, \ldots, c_{n'}) \in \mathcal{C}'\}$$

In particular, if G' is a generator matrix of $\mathcal{C}'$, then a generator matrix of $\rho_{n' \to n}(\mathcal{C}')$ is formed of the n first columns of G' and its $k = k' - (n' - n)$ first rows while a generator matrix of $\pi_{n' \to n}(\mathcal{C}')$ is formed of the n first columns of G'.

In Proposition 2 below, we establish that any code $(g)_{n,\theta}$ which is not θ-constacyclic is a shortened θ-constacyclic code.

Proposition 2 *Let $\mathcal{C} = (g)_{n,\theta}$ be a module θ-code (with $g_0 \neq 0$) which is not θ-constacyclic, then $\mathcal{C}$ is a shortened θ-constacyclic code :*

$$\exists n' > n, \exists a' \in \mathbb{F}_q^* \text{ such that } \mathcal{C} = \rho_{n' \to n}((g)^{a'}_{n',\theta})$$

PROOF. Let $\mathcal{C} = (g)_{n,\theta}$ be a module θ-code (with $g_0 \neq 0$) which is not θ-constacyclic. Then for all $n' > n$, $\mathcal{C} = \rho_{n' \to n}((g)_{n',\theta})$. It remains to prove that there exists $n' > n$ such that $\mathcal{C} = \rho_{n' \to n}((g)^{a'}_{n',\theta})$ for some $a' \in \mathbb{F}_q^*$ i.e. that there exists $n' > n$ such that g divides on the right $X^{n'} - a'$ for some $a' \in \mathbb{F}_q^*$.

From Theorem 15 in [9], g is a right divisor of a central element $f = b_0 + \ldots + b_s X^{s \cdot m} \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$ (cf. proof of Lemma 10 in [3]). As $g_0 \neq 0$, we can assume $b_0 \neq 0$. As $(\mathbb{F}_q)^\theta[X^{|\theta|}]$ is a commutative subring of $(\mathbb{F}_q)^\theta[X]$ and $b_0 \neq 0$, the central element f divides some polynomial $X^{n'} - 1$ in the commutative polynomial ring $(\mathbb{F}_q)^\theta[X]$. Let h be the polynomial in $(\mathbb{F}_q)^\theta[X]$ such that $X^{n'} - 1 = h \times f$ where the multiplication $\times$ is done in the commutative polynomial ring $(\mathbb{F}_q)^\theta[X]$. Since the coefficients are all in the fixed field of θ, we get $X^{n'} - 1 = h \cdot f$ in $\mathbb{F}_q[X;\theta]$. So f is a right divisor of $X^{n'} - 1$ in $\mathbb{F}_q[X;\theta]$ and by transitivity, we get that g divides $X^{n'} - 1$ on the right in $\mathbb{F}_q[X;\theta]$. ∎

3 Duals of module θ-codes over $\mathbb{F}_q$

To characterize the duals of module θ-codes, we will introduce the notion of the skew reciprocal polynomial of a polynomial.

Definition 3 *The* skew reciprocal polynomial *of* $h = \sum_{i=0}^{k} h_i\ X^i \in \mathbb{F}_q[X;\theta]$ *of degree* k *is defined as*

$$h^* = \sum_{i=0}^{k} X^{k-i} \cdot h_i = \sum_{i=0}^{k} \theta^i(h_{k-i})\ X^i$$

In order to describe the property of the skew reciprocal polynomial we need the following morphism of rings ([8], Lemma 5):

$$\begin{array}{rcl} \Theta\colon \mathbb{F}_q[X;\theta] & \to & \mathbb{F}_q[X;\theta] \\ \sum a_i X^i & \mapsto & \sum \theta(a_i) X^i \end{array}$$

Lemma 1 *Let* $f \in \mathbb{F}_q[X;\theta]$ *be a skew polynomial of degree* n *such that* $f = h \cdot g$*, where* h *and* g *are skew polynomials of degrees* k *and* $n - k$*. Then*

1. $f^* = \Theta^k(g^*) \cdot h^*$
2. $(f^*)^* = \Theta^n(f)$

Proof. Let $f = \sum_{i=0}^{n} f_i\ X^i, g = \sum_{i=0}^{r} g_i\ X^i$ and $h = \sum_{i=0}^{k} h_i\ X^i \in \mathbb{F}_q[X;\theta]$ be skew polynomials of degrees n, r, k with $n = k + r$.

1. For $l \in \{0, \ldots, n\}$, the l-th coefficient of f is

$$f_l = \sum_{\substack{i+j=l \\ 0 \leq i \leq k \\ 0 \leq j \leq r}} h_i\ \theta^i(g_j)$$

So the l-th coefficient of f^* (defined by $f_l^* = \theta^l(f_{n-l})$) is

$$\begin{array}{rcl} f_l^* & = & \displaystyle\sum_{\substack{i+j=n-l \\ 0 \leq i \leq k \\ 0 \leq j \leq r}} \theta^l(h_i)\ \theta^{l+i}(g_j) \qquad = \displaystyle\sum_{\substack{k-i+r-j=n-l \\ 0 \leq k-i \leq k \\ 0 \leq r-j \leq r}} \theta^l(h_{k-i})\ \theta^{l+k-i}(g_{r-j}) \\ & = & \displaystyle\sum_{\substack{i+j=l \\ 0 \leq i \leq k \\ 0 \leq j \leq r}} \theta^j(\theta^i(h_{k-i}))\ \theta^k(\theta^j(g_{r-j}))) \quad = \quad \displaystyle\sum_{\substack{i+j=l \\ 0 \leq i \leq k \\ 0 \leq j \leq r}} \theta^k(g_j^*)\ \theta^j(h_i^*) \end{array}$$

which proves that $f^* = \Theta^k(g^*) \cdot h^*$.

2. $(f^*)^* = \sum_{i=0}^{n} \theta^i(f^*_{n-i})\, X^i = \sum_{i=0}^{n} \theta^i(\theta^{n-i}(f_i))\, X^i = \Theta^n(f)$

■

Remark 1 *One can also define the skew reciprocal polynomial as $h^* = X^k \cdot \varphi(h)$ where φ is the map from $\mathbb{F}_q[X;\theta]$ to its right field of fractions $\mathbb{F}_q(X;\theta)$ defined by $\varphi(\sum a_i X^i) = \sum X^{-i} a_i$. This map is an anti-morphism (Corollary 18 of [3]) and enables to prove the point 1 of the previous lemma. We do not use it here because we have the purpose to define the skew reciprocal polynomial more generally over rings (section 5) without having to consider any field of fractions.*

According to Theorem 8 of [4], the dual code of a module θ-code is a module θ-code if and only if there exists a $b \in \mathbb{F}_q^*$ such that g divides $X^n - b$ *on the left*. For such a code to be a θ-constacyclic code, it must also divide some polynomial $X^n - a$ *on the right*. The following result allows to show that such a polynomial $X^n - a$ must exist:

Lemma 2 *Let $k \leq n$ be integers, let g and h be elements of $\mathbb{F}_q[X;\theta]$ such that $\deg(g) = n-k$ and $\deg(h) = k$.*

1. *For $b \in \mathbb{F}_q^*$, if the order of θ divides n then $X^n - b = g \cdot h \Leftrightarrow X^n - b = h \cdot g$.*
2. *For $b \in \mathbb{F}_q^*$, if g and h are monic then $X^n - b = g \cdot h \Leftrightarrow X^n - \theta^k(b) = \Theta^n(h) \cdot g$.*
3. *For $b \in \mathbb{F}_q^*$, g is a left divisor of $X^n - b$ if and only if g is a right divisor of $X^n - a$ where $a\theta^k(\lambda) = \theta^k(b)\, \theta^{k-n}(\lambda)$ and λ is the leading coefficient of g.*

PROOF.

1. If the order of θ divides n, then X^n is a central element and $X^n \cdot g = g \cdot X^n$. Therefore

$$X^n - b = g \cdot h \Rightarrow g \cdot X^n - b\, g = (g \cdot h) \cdot g \Rightarrow g \cdot (X^n - h \cdot g) = b\, g$$

Comparing the degrees we see that $X^n - h \cdot g$ is a constant b'. From the lowest coefficient we obtain $g_0\, b' = g_0\, b$. Since by assumption $g_0 \neq 0$ (because $b \neq 0$), we obtain $b = b'$.

The opposite direction is similar.

2. Suppose that h is monic and that $X^n - b = g \cdot h$. Multiplying this equality on the left by $\Theta^n(h)$ yields

$$\Theta^n(h) \cdot X^n - \Theta^n(h) \cdot b = (\Theta^n(h) \cdot g) \cdot h$$

As $\Theta(f) \cdot X = X \cdot f$, we get $X^n \cdot h - \Theta^n(h) \cdot b = (\Theta^n(h) \cdot g) \cdot h$. Therefore

$$(X^n - \Theta^n(h) \cdot g) \cdot h \;\; = \;\; \Theta^n(h) \cdot b \qquad (1)$$

showing that h is a right divisor of $\Theta^n(h) \cdot b$. As $\deg(h) = \deg(\Theta^n(h) \cdot b)$, there exists an a in $\mathbb{F}_q^*$ such that $ah = \Theta^n(h) \cdot b$. The polynomial $ah - \Theta^n(h) \cdot b$ is zero and therefore, since h is monic, its leading term $a - \theta^k(b)$ must vanish. Replacing a by $\theta^k(b)$ in (1) gives $(X^n - \Theta^n(h) \cdot g - \theta^k(b)) \cdot h = 0$. As h is monic, we get $X^n - \theta^k(b) = \Theta^n(h) \cdot g$.

Conversely, suppose that h is monic and $X^n - a = \Theta^n(h) \cdot g$. Then g is also monic and applying the above result we obtain $X^n - \theta^{n-k}(\theta^k(b)) = \Theta^n(g) \cdot \Theta^n(h)$, i.e. $\Theta^n(X^n - b) = \Theta^n(g \cdot h)$ which implies that $X^n - b = g \cdot h$.

3. Let G in $\mathbb{F}_q[X;\theta]$ be the monic skew polynomial defined by $g = \lambda\, G$.
   Suppose that g divides on the left $X^n - b$ for some b in $\mathbb{F}_q^*$. Then G divides on the left the polynomial $1/\lambda\ (X^n - b) = (X^n - b\ \theta^{-n}(\lambda)/\lambda) \cdot \theta^{-n}(1/\lambda)$ so G divides on the left $X^n - b\ \theta^{-n}(\lambda)/\lambda$. As G is monic, according to the previous point, G divides on the right $X^n - a$ where $a = \theta^k(b\ \theta^{-n}(\lambda)/\lambda)$ and $g = \lambda\, G$ also divides on the right $X^n - a$.

   Conversely, suppose that g divides on the right $X^n - a$ for some a in $\mathbb{F}_q^*$, then G also divides $X^n - a$ on the right and, as G is a monic polynomial, according to the point 2 of the lemma, it divides also $X^n - \theta^{-k}(a)$ on the left. So g divides on the left $\lambda\ (X^n - \theta^{-k}(a)) = (X^n - \lambda\ \theta^{-k}(a)/\theta^{-n}(\lambda)) \cdot \theta^{-n}(\lambda)$ hence g divides on the left $X^n - b$ where $b = \lambda\ \theta^{-k}(a)/\theta^{-n}(\lambda)$.

■

The following theorem is a generalization of Theorem 8 of [4] where duality means duality for the Euclidean scalar product. For $p = \sum p_i\ X^i, q = \sum q_i\ X^i \in \mathbb{F}_q[X;\theta]$ of degree $\leq n$ we will denote $< p, q >= \sum_{i=0}^{n} p_i q_i$.

Theorem 1 *Let $k \leq n$ be integers, $g = X^{n-k} + \sum_{i=0}^{n-k-1} g_i X^i \in \mathbb{F}_q[X;\theta]$ with constant term $g_0 \neq 0$ and $\mathcal{C}$ be the module θ-code $(g)_{n,\theta}$ of length n generated by g. The dual $\mathcal{C}^\perp$ of $\mathcal{C}$ is also a module θ-code generated by a polynomial of degree k with constant term $\neq 0$ if and only if $\mathcal{C}$ is a θ-constacyclic code, i.e. $\exists a \in \mathbb{F}_q^*$ such that $\mathcal{C} = (g)_{n,\theta}^a$. In this case $\mathcal{C}^\perp$ is a θ-constacyclic code generated by h^**

$$\mathcal{C}^\perp = (h^*)_{n,\theta}^{a^*}$$

where $h \in \mathbb{F}_q[X;\theta]$ is such that $X^n - \theta^{-k}(a) = g \cdot h$ and where $a^* = \dfrac{\theta^n(g_0)}{g_0\ \theta^{n-k}(a)}$.

Proof. Let $\mathcal{C} = (g)_{n,\theta}$ be the module θ-code generated by g with $g_0 \neq 0$ and g monic of degree $n - k$.

- Suppose that $\mathcal{C}$ is θ-constacyclic and let $a \in \mathbb{F}_q^*$ be such that $\mathcal{C} = (g)_{n,\theta}^a$. As g divides on the right $X^n - a$ and as g is monic, according to the second statement of Lemma 2, g divides on the left $X^n - b$ where $b = \theta^{-k}(a)$. Let $h \in \mathbb{F}_q[X;\theta]$ be the corresponding right factor, i.e. $g \cdot h = X^n - b$. According to the proof of Theorem 8 of [4], we have $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$,

$$< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) \tag{2}$$

  and, as $k+j-i \in \{1, \ldots, n-1\}$, we get $< X^i \cdot g, X^j \cdot h^* >= 0$, so that $\mathcal{C}^\perp = (h^*)_{n,\theta}$. Let us now prove that $\mathcal{C}^\perp = (h^*)_{n,\theta}^{a^*}$, i.e. that h^* divides on the right $X^n - a^*$. According to Lemma 1, $\Theta^{n-k}(h^*) \cdot g^* = (X^n - b)^* = 1 - X^n \cdot b = (1/b - X^n) \cdot b$, so $h^* \cdot \Theta^{k-n}(g^*) = \Theta^{k-n}(X^n - 1/b) \cdot \theta^{k-n}(-b)$ and h^* divides on the left $\Theta^{k-n}(X^n - 1/b) = X^n - \theta^{k-n}(1/b)$. Let λ be the leading term of h^* i.e. $\lambda = \theta^k(h_0) = -a/\theta^k(g_0)$. According to Lemma 2, h^* divides on the right $X^n - a^*$ where $a^* = \ \theta^{-k}(\lambda)\ \theta^{n-k}(1/\lambda)\ 1/b = \dfrac{\theta^n(g_0)}{g_0\ \theta^{n-k}(a)}$, which proves that $\mathcal{C}^\perp = (h^*)_{n,\theta}^{a^*}$ is θ-constacyclic.

- Conversely, suppose that $\mathcal{C}^\perp$ is a module θ-code and let $p \in \mathbb{F}_q[X;\theta]$ be its monic generator polynomial. Then $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}, < X^i \cdot g, X^j \cdot p >=$

0. Let h be the skew polynomial defined by $h = \Theta^{-k}(p^*)$, then $h^* = \Theta^{-k}(p^{**}) = p$ (according to Lemma 1). Hence according to (2) $< X^i \cdot g, X^j \cdot p >=< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i})$ and $g \cdot h$ is a polynomial of degree n whose terms of degrees in $\{1, \ldots, n-1\}$ vanish. Consequently there exists some $b \in \mathbb{F}_q^*$ such that $g \cdot h = X^n - b$ ($b \neq 0$ because $h_0 = 1$ and $g_0 \neq 0$) and according to Lemma 2, g divides on the right $X^n - \theta^k(b)$ which implies that $\mathcal{C}$ is θ-constacyclic.

■

We can now prove a refined version of the conjecture stated in [4] :

Corollary 1 *Consider $\theta \in Aut(\mathbb{F}_q)$, $R = \mathbb{F}_q[X;\theta]$ and $g \in R$ monic with nonzero constant term g_0. If the module θ-code $(g)_{n=2k,\theta}$ is self-dual then $(g)_{n=2k,\theta}$ is necessarily a θ-constacyclic code where g divides $X^n - a$ on the right and $a \in \mathbb{F}_q^*$ is defined by*

$$a\ \theta^k(a)\ g_0 = \theta^{2k}(g_0)$$

PROOF. Let $\mathcal{C} = (g)_{n=2k,\theta}$ be a self-dual module θ-code. According to Theorem 1, $\mathcal{C}$ is a θ-constacyclic code and there exists some $b \in \mathbb{F}_q^*$ such that g divides $X^n - b$ on the left and $X^n - a$ on the right, where $a = \theta^k(b)$. The generator polynomial of $\mathcal{C}^\perp$ is h^* where $g \cdot h = X^n - b$ and h^* is a right factor of $X^n - a^*$, where $a^* = \frac{\theta^{2k}(g_0)}{g_0\ \theta^k(a)}$. As $\mathcal{C} = \mathcal{C}^\perp$, we get $g = 1/\theta^k(h_0)\ h^*$ so h^* divides on the right $X^n - a$. As it divides $X^n - a^*$ on the right, it divides $a - a^*$ on the right, so $a = a^*$ which means $a\ \theta^k(a)\ g_0 = \theta^{2k}(g_0)$. ■

Note that if the length of a self-dual module θ-code is a multiple of the order of θ, then $a\ \theta^k(a)\ g_0 = \theta^{2k}(g_0) \Rightarrow a\ \theta^k(a) = 1$. Furthermore, according to Lemma 2 point 1, g divides on the right and on the left both $X^n - a$ and $X^n - \theta^{-k}(a)$ so $a = \theta^{-k}(a)$ hence $a^2 = 1$ and a self-dual module θ-code whose length is a multiple of the order of θ is either θ-cyclic or θ-negacyclic. In particular, over $\mathbb{F}_4$, self-dual module θ-codes are θ-cyclic (Proposition 13 of [4]) and over $\mathbb{F}_{p^2}$ with p a prime number, they are either θ-cyclic or θ-negacyclic.

The above theorem can also be restated in terms of the group of semi-linear automorphisms of the module θ-code thanks to Proposition 1.

Corollary 2 *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear code of length n having a generator matrix of the form*

$$\begin{pmatrix} g_0 & \ldots & g_{n-k-1} & g_{n-k} & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \ldots & \theta(g_{n-k-1}) & \theta(g_{n-k}) & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \ldots & 0 & \theta^{k-1}(g_0) & \ldots & \theta^{k-1}(g_{n-k-1}) & \theta^{k-1}(g_{n-k}) \end{pmatrix}.$$

The dual of $\mathcal{C}$ has a generator matrix of the same form

$$\begin{pmatrix} h_0^* & \ldots & h_{k-1}^* & h_k^* & 0 & \ldots & 0 \\ 0 & \theta(h_0^*) & \ldots & \theta(h_{k-1}^*) & \theta(h_k^*) & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \ldots & 0 & \theta^{n-k-1}(h_0^*) & \ldots & \theta^{n-k-1}(h_{k-1}^*) & \theta^{n-k-1}(h*_k) \end{pmatrix}$$

if and only if $\mathcal{C}$ *is invariant under the semi-linear map* $\sigma_a \circ \Theta$ *where* $a \in \mathbb{F}_q^*$, $\Theta : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *is defined by* $\Theta((c_0, \ldots, c_{n-1})) = (\theta(c_0), \ldots, \theta(c_{n-1}))$ *and* σ_a *is an* $\mathbb{F}_q$*-linear map of* $\mathbb{F}_q^n$ *whose matrix is*

$$\begin{pmatrix} 0 & \cdots & 0 & 0 & a \\ 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

In this case $h^* = \sum_{i=0}^{k} h_i^* X^i \in \mathbb{F}_q[X;\theta]$ *is the skew reciprocal polynomial of* $h \in \mathbb{F}_q[X;\theta]$ *having the property that* $X^n - \theta^{-k}(a) = g \cdot h$ *in* $\mathbb{F}_q[X;\theta]$.

Since there are much more factors of $X^n - a$ in the nonunique factorization ring $\mathbb{F}_q[X;\theta]$ than in the commutative case, there are many codes of the above form that are invariant under the semi-linear map $\sigma_a \circ \theta$.

We have established that the dual of a module θ-code $\mathcal{C}$ is a module θ-code if and only if $\mathcal{C}$ is θ-constacyclic. If the code is not θ-constacyclic, it is still possible to characterize the dual as the punctured code of a θ-constacyclic code :

Proposition 3 *Let* $k \leq n$ *be integers,* $g \in \mathbb{F}_q[X;\theta]$ *of degree* $n-k$ *with nonzero constant term and* $\mathcal{C}$ *be the module* θ*-code of length* n *generated by* g*. Let us assume that* $\mathcal{C}$ *is not* θ*-constacyclic, then* $\mathcal{C}^\perp$ *is a punctured code of a* θ*-constacyclic code. More precisely,* $\exists (n', a') \in \mathbb{N}^* \times \mathbb{F}_q^*$ *such that :*

$$n' > n \quad \text{and} \quad \mathcal{C}^\perp = \pi_{n' \to n}\left(\mathcal{C}'^\perp\right)$$

where $\mathcal{C}' = (g)_{n',\theta}^{a'}$ *is a* θ*-constacyclic code and* $\mathcal{C} = \rho_{n' \to n}(\mathcal{C}')$.

Proof. Let $\mathcal{C} = (g)_{n,\theta}$ be a module θ-code (with $g_0 \neq 0$) which is not θ-constacyclic. According to Proposition 2, there exists $(n', a') \in \mathbb{N}^* \times \mathbb{F}_q^*$ such that $n' > n$ and $\mathcal{C} = \rho_{n' \to n}(\mathcal{C}')$ where $\mathcal{C}' = (g)_{n',\theta}^{a'}$. For $c \in \mathbb{F}_q^n$, $c \in \mathcal{C}$ is equivalent to

$$\begin{aligned} & (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in \mathcal{C}' \\ \Leftrightarrow \quad & \forall c' \in \mathcal{C}'^\perp, < (c_0, \ldots, c_{n-1}, 0, \ldots, 0), (c'_0, \ldots, c'_{n-1}, c'_n, \ldots, c'_{n'-1}) >= 0 \\ \Leftrightarrow \quad & \forall c' \in \mathcal{C}'^\perp, < (c_0, \ldots, c_{n-1}), (c'_0, \ldots, c'_{n-1}) >= 0 \end{aligned}$$

so the words of $\mathcal{C}$ are orthogonal to the words of $\pi_{n' \to n}(\mathcal{C}'^\perp)$ and $\mathcal{C}^\perp = \pi_{n' \to n}(\mathcal{C}'^\perp)$.

■

One can deduce an expression for the parity check matrix of a module θ-code (which generalizes the result of Corollary 9 [4] for θ-constacyclic codes).

Corollary 3 (Parity check matrix of a module θ-code) *Let* $k \leq n$ *be integers,* $g \in \mathbb{F}_q[X;\theta]$ *be of degree* $n-k$ *with a nonzero constant term and* $\mathcal{C} = (g)_{n,\theta}$ *be the module* θ*-code of length* n *generated by* g*. A parity check matrix of* $\mathcal{C}$ *is the* $(n-k) \times n$ *matrix* $H_{g,n,\theta}$ formed by the n first columns *of the* $(n-k) \times n'$ *matrix:*

$$\begin{pmatrix} h_{n'-n+k} & \cdots & & \theta^{n'-n+k}(h_0) & 0 & \cdots & 0 \\ 0 & \theta(h_{n'-n+k}) & \cdots & \cdots & \theta^{n'-n+k+1}(h_0) & \cdots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & \theta^{n-k-1}(h_{n'-n+k}) & \cdots & & \theta^{n'-1}(h_0) \end{pmatrix}$$

where $n' \geq n$ and $h \in \mathbb{F}_q[X;\theta]$ are such that $X^{n'} - g \cdot h = b' \in \mathbb{F}_q^*$.

4 Parity check matrix of module (θ, δ)-codes over a field

For $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ a θ-derivation is a map $\delta : \mathbb{F}_q \to \mathbb{F}_q$ such that for all a and b in $\mathbb{F}_q$:

$$\begin{aligned} \delta(a+b) &= \delta(a) + \delta(b) \\ \delta(ab) &= \delta(a)b + \theta(a)\delta(b). \end{aligned}$$

For a finite field $\mathbb{F}_q$, all θ-derivations are of the form $\delta_\beta(a) = \beta\,(\theta(a) - a)$ where $\beta \in \mathbb{F}_q$ and are therefore uniquely determined by $\beta \in \mathbb{F}_q$. According to [7] the most general skew polynomial rings in the variable X (such that $\deg(f \cdot g) = \deg(f) + \deg(g)$) over $\mathbb{F}_q$, whose elements are written $\sum_{i=0}^{n} a_i X^i$, are defined with the usual addition of polynomials and a multiplication that follows the commuting rule $X \cdot a = \theta(a)X + \delta(a)$. We note the resulting ring $\mathbb{F}_q[X;\theta,\delta]$ and call it skew polynomial ring again. It is a left and right Euclidean ring in which left and right gcd and lcm exist [7].

Definition 4 ([5]) *Consider $R = \mathbb{F}_q[X;\theta,\delta]$ and let $f \in R$ be of degree n. A* module (θ,δ)-code *$\mathcal{C}$ is a left R-submodule $Rg/Rf \subset R/Rf$ in the basis $1, X, \ldots, X^{n-1}$ where g is a right divisor of f in R. The length of the code is $n = \deg(f)$ and its dimension is $k = \deg(f) - \deg(g)$, we say that the code $\mathcal{C}$ is of type $[n,k]_q$. If the minimal distance of the code is d, then we say that the code $\mathcal{C}$ is of type $[n,k,d]_q$. We denote this code $\mathcal{C} = (g)_{n,\theta,\delta}$.*

A change of variable $Z = X + \beta$ transforms the ring $\mathbb{F}_q[X;\theta,\delta]$ into a pure automorphism ring $\mathbb{F}_q[Z;\theta]$. A generator matrix of a module (θ,δ)-code $(g)_{n,\theta,\delta}$ can be related to the generator matrix of a module θ-code $(\tilde{g})_{n,\theta}$ (cf. [5]) :

$$G_{g,n,\theta,\delta} = G_{\tilde{g},n,\theta} \times A_{n,n}(\beta),$$

where $\tilde{g} = \sum_{i=0}^{n-k} \tilde{g}_i Z^i \in \mathbb{F}_q[Z;\theta]$ is such that $\sum_{i=0}^{n-k} g_i X^i = \sum_{i=0}^{n-k} \tilde{g}_i (X+\beta)^i$ and $A_{n,n}(\beta)$ is a lower unit triangular $n \times n$ matrix over $(\mathbb{F}_q)^\theta(\beta)$ whose entries $a_{i,j}$ $(j < i)$ are given by $a_{i+1,j+1} = \theta(a_{i,j}) + \beta\theta(a_{i,j+1})\,(1 < j < i)$, $a_{i+1,1} = \beta\theta(a_{i,1})\,(1 < j)$.

More generally, we can give a parity check matrix for module (θ,δ)-codes.

Corollary 4 (Parity check matrix of a module (θ,δ)-code) *Let $k \leq n$ be integers, let $g \in \mathbb{F}_q[X;\theta,\delta]$ be of degree $n-k$ with constant term $\neq 0$. Let $\mathcal{C} = (g)_{n,\theta,\delta}$ be the module (θ,δ)-code of length n generated by g. A parity check matrix of $\mathcal{C}$ is the $(n-k) \times n$ matrix*

$$H_{g,n,\theta,\delta} = H_{\tilde{g},n,\theta} \times (A_{n,n}(\beta)^{-1})^T$$

where $H_{\tilde{g},n,\theta}$ is the parity check matrix of the code $(\tilde{g})_{n,\theta}$ defined in Corollary 3 and $\tilde{g}$ is defined in $\mathbb{F}_q[Z;\theta]$ by $\sum_{i=0}^{n-k} g_i\, X^i = \sum_{i=0}^{n-k} \tilde{g}_i\, Z^i$ with $Z = X + \beta$.

On can find examples which show that the conjecture (Corollary 1) is not true for module (θ,δ)-codes defined over finite fields so it remains to determine when the dual of a module (θ,δ)-code is a module (θ,δ)-code. In the next section we consider module θ-codes over rings.

5 Duals of module θ-codes defined over rings

The notion of θ-constacyclic codes over Galois rings appears in [2] where the notion of module θ-codes is extended to module θ-codes over a ring A with zero divisors. The skew polynomial ring $A[X;\theta]$ is nonprincipal and we restrict ourselves to codes defined by principal modules generated by polynomials whose leading terms are invertible.

Definition 5 *Let θ be an automorphism of the finite ring A and $R = A[X;\theta]$. A* module θ-code *$\mathcal{C}$ is a left R-submodule $Rg/Rf \subset R/Rf$ in the basis $1, X, \ldots, X^{n-1}$ where $f \in R$ is monic and g is a monic right divisor of f in R. The length of the code is $n = \deg(f)$ and its rank is $k = \deg(f) - \deg(g)$, we say that the code $\mathcal{C}$ is of type $[n,k]_q$. If the minimal distance of the code is d, then we say that the code $\mathcal{C}$ is of type $[n,k,d]_q$. We denote this code $\mathcal{C} = (g)_{n,\theta}$.*
If there exists an $a \in A$ such that a is invertible in A and g divides $X^n - a$ on the right then the code $(g)_{n,\theta}$ is θ-constacyclic. *We will denote it $(g)^a_{n,\theta}$. If $a = 1$, the code is* θ-cyclic *and if $a = -1$, it is* θ-negacyclic.

Similar to the case of a field we neglect module θ-codes where the first entries of any code word is always zero by assuming that the constant term of the generator polynomial g is nonzero. One verifies that the skew reciprocal polynomial is still defined, that the application Θ is still a morphism of rings and therefore that the Lemma 1 remains true. Furthermore Lemma 2 remains true if we assume that the leading term of g is invertible in A. Consequently, Theorem 1 remains valid if one assumes that the constant term of the generator polynomial g of the code (or of the polynomial h) is invertible.

Corollary 5 *Consider a finite ring A, $\theta \in Aut(A)$ and let g be a monic skew polynomial of $A[X;\theta]$ with a constant term g_0 invertible in A. If the module θ-code $(g)_{n,\theta}$ is self-dual then it is necessarily a θ-constacyclic code where g divides $X^n - a$ on the right and*

$$a\ \theta^k(a)\ g_0 = \theta^{2k}(g_0)$$

6 Self-dual Euclidean module skew codes of length 2^s over $\mathbb{F}_4$

In [1], [6] the authors construct cyclic codes of length $n = p^\alpha$ over $\mathbb{F}_{p^m}$ (p prime number) whose rates are $\geq R$ (R fixed) and whose minimal distances d_{min} are bounded by some value which is independent of α (which implies that d_{min}/n tends to 0 when n increases to infinity).

In $\mathbb{F}_4[X]$, the polynomial $X^{2^s} + 1 = (X+1)^{2^s}$ has only one factor of degree 2^{s-1}, $g = (X+1)^{2^{s-1}}$, and it therefore generates the unique $[2^s, 2^{s-1}]_4$ cyclic code. Its minimal distance is 2 and it is a self-dual code.

In $\mathbb{F}_4[X;\theta]$, the polynomial $X^{2^s} + 1$ has many factors on the right of degree 2^{s-1} ($X^2 + 1$ has three factors of degree 1 on the right, $X^4 + 1$ has seven factors of degree 2 on the right, ...) but it seems that only two of them generate self-dual θ-cyclic (noncyclic) codes (according to experimental results of [3] obtained for $s = 2, 3, 4, 5$).

In this section, we give a partial explanation to this experimental result. Namely, we construct two sequences of self-dual θ-cyclic codes (which are not cyclic) over $\mathbb{F}_4$ of length 2^s (with rate 1/2) and with minimal distance 4. We conjecture that there is no other $[2^s, 2^{s-1}]_4$ self-dual module θ-codes.

Theorem 2 *For $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $s \in \mathbb{N}, s \geq 2$ and $i \in \{1, 2\}$, the polynomial $g_{s,i} \in \mathbb{F}_4[X; \theta]$ defined by*

$$g_{s,i} = (X + \alpha^i) \cdot (X + 1)^{2^{s-1}-1}$$

generates a self-dual θ-cyclic code (which is not cyclic) of length 2^s over $\mathbb{F}_4$ with minimal distance $d_{s,i}$ satisfying $d_{2,i} = 3$ and $d_{s,i} = 4$ if $s \geq 3$.

Proof. Let s be an integer ≥ 2. As $g_{s,2} = \Theta(g_{s,1})$, $g_{s,1}$ generates a self-dual θ-cyclic code if and only if $g_{s,2}$ generates a self-dual θ-cyclic code. Furthermore, the minimal distances of the two codes are equal. Namely $(g_{s,2})_{n,\theta} = \{\Theta(c), c \in (g_{s,1})_{n,\theta}\}$ where $\Theta(c) = (\theta(c_0), \ldots, \theta(c_{n-1}))$. Hence in the following we will give the proof only for $i = 1$ and we will denote $g_s = g_{s,1}$.

- We first prove that g_s generates a θ-cyclic code of length 2^s. For $h_s = (X + 1)^{2^{s-1}-1} \cdot (X + \alpha^2)$ we have

$$\begin{aligned} g_s \cdot h_s &= (X + \alpha) \cdot (X + 1)^{2^{s-1}-1} \cdot (X + 1)^{2^{s-1}-1} \cdot (X + \alpha^2) \\ &= (X + \alpha) \cdot (X^2 + 1)^{2^{s-1}-1} \cdot (X + \alpha^2) \end{aligned}$$

  As $(X^2 + 1)^{2^{s-1}-1}$ is in $\mathbb{F}_2[X^2]$, the center of $\mathbb{F}_4[X; \theta]$, we get

$$g_s \cdot h_s = (X + \alpha) \cdot (X + \alpha^2) \cdot (X^2 + 1)^{2^{s-1}-1}$$

  Furthermore, $(X + \alpha) \cdot (X + \alpha^2) = X^2 + 1$ so

$$g_s \cdot h_s = (X^2 + 1)^{2^{s-1}} = X^{2^s} + 1$$

  and as the order of θ divides 2^s, according to Lemma 2, we have $h_s \cdot g_s = g_s \cdot h_s = X^{2^s} - 1$. Hence g_s generates a θ-cyclic code of length 2^s. Its dual is generated by h_s^*.

- We now prove that this code is self-dual by showing that h_s^* is a constant times g_s. We have $h_s = f_1 \cdot f_2$ where $f_1 = (X + 1)^{2^{s-1}-1}$ and $f_2 = X + \alpha^2$. According to Lemma 1,

$$h_s^* = \Theta^{2^{s-1}-1}(f_2^*) \cdot f_1^*$$

  As $f_1 = \sum_{i=0}^{2^{s-1}-1} C_{2^{s-1}-1}^i X^i = \sum_{i=0}^{2^{s-1}-1} C_{2^{s-1}-1}^{2^{s-1}-1} i X^{2^{s-1}-i}$ we have $f_1 = f_1^*$. Furthermore $f_2^* = 1 + \theta(\alpha^2)X = \alpha(X + \alpha^2)$ and $\Theta^{2^{s-1}-1} = \Theta$ so

$$h_s^* = \Theta(\alpha(X + \alpha^2)) \cdot f_1 = \alpha^2(X + \alpha) \cdot (X + 1)^{2^{s-1}-1}.$$

  Therefore $h_s^* = \alpha^2 \, g_s$.

- Let us compute the minimal distance of $(g_s)_{2^s}$. The minimal distance (computed using Magma) of $(g_2)_4$ is 3. Let s be an integer ≥ 3 and let us find a code word of weight 4 in $(g_s)_{2^s}$. The polynomial $h_{s-1} \cdot g_s$ (written in the basis $(1, X, X^2, \ldots)$) represents a code word of $(g_s)_{2^s}$ because $\deg(h_{s-1}) = 2^{s-2} < 2^{s-1}$. As $g_s = g_{s-1} \cdot (X + 1)^{2^{s-2}}$, we have

$$h_{s-1} \cdot g_s = h_{s-1} \cdot g_{s-1} \cdot (X + 1)^{2^{s-2}}$$

  As $h_{s-1} \cdot g_{s-1} = (X + 1)^{2^{s-1}}$, we get

$$h_{s-1} \cdot g_s = (X^{2^{s-1}} + 1) \cdot (X^{2^{s-2}} + 1) = X^{3 \times 2^{s-2}} + X^{2^{s-1}} + X^{2^{s-2}} + 1$$

showing that the code has a word of weight 4 and that $d_s \leq 4$.

Let us prove by induction on s that there is no code word of weight < 4 in $(g_s)_{2^s}$ for $s \geq 3$. It is true for $s = 3$ as the minimal distance of $(g_3)_8$ (computed using Magma) is equal to 4. Let s be an integer ≥ 3 and suppose that there is no code word of weight < 4 in $(g_s)_{2^s}$. If $(g_{s+1})_{2^{s+1}}$ has a code word c of weight < 4, then by definition of the code there exists a polynomial m of degree $< 2^s$ such that $c = m \cdot g_{s+1}$. As $g_{s+1} = g_s \cdot (X+1)^{2^{s-1}}$ and as the polynomial $(X+1)^{2^{s-1}}$ is central, we get

$$c = m \cdot (X+1)^{2^{s-1}} \cdot g_s$$

Let c' be the remainder in the right division of c by $X^{2^s} - 1$. As c is a right multiple of g_s, c' belongs to the θ-cyclic code $(g_s)_{2^s}$. By hypothesis, the weight of c is < 4 and for $i \in \mathbb{N}$, the remainder in the right division of X^i by $X^{2^s} - 1$ is $X^{i \bmod 2^s}$ so the weight of c' is < 4, which is impossible by induction hypothesis. So $(g_{s+1})_{2^{s+1}}$ contains no nonzero code word c of weight < 4 and its minimal distance is 4.

■

Remark 2 *The only self dual skew code of length* 2 *over* $\mathbb{F}_4$ *is* $(X+1)_2$*. It is a* $[2, 1, 2]$ *cyclic code.*

The theorem enables to construct a sequence $(\mathcal{C}_s)_{s\in\mathbb{N}}$ of self-dual θ-cyclic codes over $\mathbb{F}_4$ of length $n_s = 2^s$ which are not cyclic codes and which satisfy $\lim_{n_s\to\infty} \frac{dmin(\mathcal{C}_s)}{n_s} = 0$, namely the θ-cyclic codes generated by $g_s = (X+\alpha)\cdot(X+1)^{2^{s-1}-1}$.

Conjecture 1 *The only self-dual module* θ*-codes of length* 2^s *over* $\mathbb{F}_4$ *(with* $\theta : a \mapsto a^2$*) are the cyclic code generated by* $(X+1)^{2^{s-1}}$ *and the* θ*-cyclic codes generated by* $g_{s,1}$ *and* $g_{s,2}$*.*

One can check that this conjecture is true for $s = 6$.

References

[1] Berman, S. D. *On the theory of group codes*, Cybern., vol. 3, no. 1, pp 25-31, 1967

[2] Boucher, D., Solé, P. and Ulmer, F., *Skew Constacyclic Codes over Galois Rings*, Advances in Mathematics of Communications, 2, 273-292 (2008)

[3] Boucher, D. and Ulmer, F., *Coding with skew polynomial rings*, Journal of Symbolic Computation, 44, 1644-1656 (2009).

[4] Boucher, D. and Ulmer, F., *Codes as modules over skew polynomial rings* Lecture notes in computer science , volume = 5921 , (2009)

[5] Boucher, D. and Ulmer, F., *Linear codes using skew polynomials with automorphisms and derivations*. Prépublication IRMAR, mai 2011.

`http://hal.archives-ouvertes.fr/hal-00597127_v1/`

[6] Castagnoli G. *On the asymptotic badness of cyclic codes with block-lengths composed from a fixed set of prime factors*, Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988), Lecture Notes in Comput. Sci., 357, 164–168, 1989

[7] O. Ore, Theory of Non-Commutative Polynomials, *The Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp 480-508 (1933)

[8] L. Chaussade, P. Loidreau and F. Ulmer, *Skew codes of prescribed distance or rank*, Designs, Codes and Cryptography, 50(3), 267-284 (2009)

[9] Jacobson, N., *The theory of rings*, Publication of the AMS (1943).